



Contract No.: DAMD17-99-C-9001

Defense Healthcare Information Assurance Program (DHIAP)

DHIAP Phase I Technology Demonstration Report

Prototype for Remote Authentication Dial-In User Service (RADIUS)

ATI IPT Technical Report 00-04

April 2000

Prepared for:

U.S. Army Medical Research and Materiel Command

Fort Detrick

Frederick, Maryland 21702-5012

This work was supported by the U.S. Army Medical Research and Materiel Command under Contract No. DAMD 17-99-C-9001. The views, opinions and/or findings contained in this report are those of the authors and should not be construed as an official Department of the Army position, policy, or decision unless so designated by other documentation.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 01-04-2000		2. REPORT TYPE		3. DATES COVERED (FROM - TO) xx-xx-2000 to xx-xx-2000	
4. TITLE AND SUBTITLE DHIAP Phase I Technology Demonstration Report: Prototype for Remote Authentication Dial-In User Service (RADIUS) (ATI IPS Technical Report 00-004) Unclassified				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Crane , Lynn S. ; Melton, Lane H. ; Stinson, Jr., Jack ;				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME AND ADDRESS Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA22102				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS US Army Medical Research and Materiel Command Fort Detrick Frederick, MD21702-5012				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APUBLIC RELEASE					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The Defense Healthcare Information Assurance Program (DHIAP) involved demonstration of prototype information assurance technology to assess the impact on military Medical Treatment Facility (MTF) operations and ability to improve security of sensitive information. The prototype, developed and tested in a distributed laboratory and demonstrated at two MTFs within a region, is a system that meets the Remote Authentication Dial-In User Service (RADIUS) standard. This report describes the development and trials of the technology and provides an analysis of alternative					
15. SUBJECT TERMS IATAC COLLECTION; information security; information technology; information assurance; computer security; healthcare information systems; RADIUS; network access security; access control; dial-in					
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT Public Release	18. NUMBER OF PAGES 50	19. NAME OF RESPONSIBLE PERSON Fenster, Lynn lfenster@dtic.mil	
a. REPORT Unclassified		b. ABSTRACT Unclassified		c. THIS PAGE Unclassified	
				19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007	
				Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39.18	

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 4/1/2000	3. REPORT TYPE AND DATES COVERED Report 4/1/2000	
4. TITLE AND SUBTITLE DHIAP Phase I Technology Demonstration Report: Prototype for Remote Authentication Dail-In User Service (RADIUS) (ATI IPS Technical Report 00-004)			5. FUNDING NUMBERS	
6. AUTHOR(S) Crane, Lynn S.; Melton, Lane H.; Stinson Jr, Jack				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) US Army Medical Research and Materiel Command For Detrick, Frederick, MD 21702-5012			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) The Defense Healthcare Information Assurance Program (DHIAP) involved demonstration of prototype information assurance technology to assess the impact on military Medical Treatment Facility (MTF) operations and ability to improve security of sensitive information. The prototype, developed and tested in a distributed laboratory and demonstrated at two MTFs within a region, is a system that meets the Remote Authentication Dial-In User Service (RADIUS) standard. This report describes the development and trials of the technology and provides an analysis of alternative				
14. SUBJECT TERMS IATAC Collection, information security, information technology, information assurance, computer security, healthcare information systems, RADIUS, network access security, access control, dial-in			15. NUMBER OF PAGES 47	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED	



DHIAP Phase I Technology Demonstration Report
Prototype for Remote Authentication Dial-In User Service (RADIUS)

ATI IPS Technical Report 00-04

Authors:

Lynn S. Crane, ATI
Lane H. Melton, ATI
Jack A. Stinson Jr., ATI

Contributors:

Archie D. Andrews, ATI
Forrest V. Schwengels II, LMES
Thornton C. White, ADL

PREFACE

This report was prepared by the staff of the Information Protection Technology group of the Advanced Technology Institute as part of the Defense Healthcare Information Assurance Program (DHIAP). The DHIAP work is supported by the U.S. Army Medical Research and Materiel Command. As noted, the views, opinions and/or findings contained in this report are those of the authors and should not be construed as official Department of the Army position, policy or decision.

This report on the DHIAP Technology Demonstration, Prototype for Remote Authentication Dial-In User Service (RADIUS), is prepared as a report on the selection, testing, installation, and transition of the prototype demonstration to operational Medical Treatment Facilities (MTF). It is written for MEDCOM and MTF management based on lessons learned and experiences gained during the course of designing, installing, and testing RADIUS compliant systems in the laboratory and at operational sites. It is written as an aid to understanding the basis of the RADIUS technology, the technology prototyped and demonstrated at the laboratory and the test sites, potential implementation alternatives, and the costs in dollars and personnel resources of providing services demonstrated in this prototype.

The information contained herein is drawn from many sources including vendors' literature, extensive correspondence and discussion with vendor technical representatives, MTF information management staff as well as experiences and lessons learned during the course of the installations and testing.

This report is one piece of a body of work completed during Phase I of DHIAP. The DHIAP team has published two other documents relating the work performed in Phase I of DHIAP. The *DHIAP RADIUS Supplemental Installation and Maintenance Guide (ATI Special Report IPS 00-03)* was developed as a guide for installation and configuration of the RADIUS-compliant system prototyped during the technology demonstration. It serves as a supplement to existing Cisco and Microsoft vendors' instructions. Reference to that guide should help the reader interested in technical details to understand the internal operations of the hardware and software deployed in the RADIUS-compliant systems. The *DHIAP Phase I Composite Evaluation Report (ATI Technical Report IPS TR 00-02)*, provides a compendium of the findings and recommendations of the Information Security Evaluations conducted at military MTF as part of DHIAP Phase I. This report outlines vulnerabilities identified and provides subject-specific recommendations for remedial actions. It also outlines recommended crosscutting activities that address such organizational focus areas as policy definition, procedure development, and training. This report on the evaluations provides insight into areas of potential security vulnerabilities that are not addressed by this technology demonstration.

Ms. Lynn Crane was the principal author and overall coordinator for this report, with significant technical input from Mr. Lane Melton and Dr. Jack Stinson. Other contributors included Mr. Forrest Schwengels of the Advanced Computing Technology staff of Lockheed Martin Energy Systems, Mr. Thornton White of Arthur D. Little, Inc., and numerous members of the Cisco Technical Staff. Mr. Archie Andrews assisted in editing the report. Sarah Hartline typed and revised the many drafts of the guide and prepared the report for publication.

Archie D. Andrews

Principal Investigator, Defense Healthcare Information Assurance Program
Director, Information Protection Technology
Advanced Technology Institute

TABLE OF CONTENTS

<i>PREFACE</i>	<i>i</i>
<i>EXECUTIVE SUMMARY</i>	<i>v</i>
<i>I. INTRODUCTION</i>	<i>1</i>
DHIAP Background	1
Purpose of Report	2
Report Organization	2
Intended Audience	3
<i>II. TECHNOLOGY DEMONSTRATION</i>	<i>5</i>
Summary of DHIAP Program Activities	5
Project Participants	5
Technical Assessment	5
Prototype Design and Development	6
Selection of RADIUS as the DHIAP Demonstration Prototype	6
Prototype Design	7
Prototype Development and Evaluation.....	7
Demonstration	8
Technology Transition	8
<i>III. RESULTS AND OBSERVATIONS</i>	<i>9</i>
Minimum Configuration	10
Ease of Installation	11
Ease of Operation and Maintenance	12
Support for Remote System Users	12
Support of User Accounts	12
Support of Accounting Logs.....	13
<i>IV. RADIUS IMPLEMENTATION IN THE ARMY MEDICAL DOMAIN</i>	<i>15</i>
Technical Approach	15
Autonomous Complete RADIUS-Compliant Systems at Every Site	16
Complete System at Central Site and NAS at All Satellite Sites	16
Redundant Complete Systems and NAS at Remaining Satellite Sites	17
Note on Consequences of a Non-Functional NAS.....	18
Program Management and Programmatic	18
<i>APPENDICES</i>	<i>23</i>
Appendix A - Reference Materials	25
Appendix B - Army Dial-in Modem Standards and Policy	27
Appendix C - Overview of IETF Internet Standard Protocol for RADIUS	29
Appendix D - DHIAP Prototype Implementation	31

DHIAP PHASE I TECHNOLOGY DEMONSTRATION
PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

Equipment Configuration..... 31

Processing Flow..... 31

Appendix E - Acronyms.....35

Report Documentation Page, Form OMB No. 0704-0188.....37

TABLE OF FIGURES

Figure 1 - Summary of DHIAP Phase I Activities	5
Figure 2 - Criteria for Prioritizing Information	6
Figure 3 - Army and MTF Requirements for the DHIAP Prototype	7
Figure 4 - Technology Alternatives Reviewed by the DHIAP Team	7
Figure 5 - DHIAP's Use of Region's NT Structure.....	12
Figure 6 - Typical Group Privileges for an MTF	13
Figure 7 - <i>Autonomous</i> Configuration – Complete Systems at All Sites.....	15
Figure 8 - <i>Central</i> Configuration – Complete System at One Site and NAS-Only at Remaining Sites.....	15
Figure 9 - <i>Redundant</i> Configuration – Complete System at Two Sites, NAS-Only at Remaining Sites.....	16
Figure 10 - Authentication by 2 nd Site AAA Server when Primary AAA Server is Not Functioning	16
Figure 11 - Loss of Service to Users when Site NAS is Down	17
Figure D1 - Components of the DHIAP Demonstration's RADIUS Compliant System	28
Figure D2 - AUTHENTICATION/ACCOUNTING for Remote User Access to Network Resources	30
Figure D3 - AUTHORIZATION/ACCOUNTING for Remote User Access to Network Resources	30

TABLE OF TABLES

Table 1 - Army Dial-In Users Requirements vs. DHIAP RADIUS system.....	6
Table 2 - MTF-Requested Features of the DHIAP RADIUS Compliant System	10
Table 3 - DHIAP RADIUS Hardware/Software Components	11
Table 4 - Sample Costs for DHIAP Technology Options	18
Table 5 - Task, Training and Staffing Requirements to support the DHIAP Technology	20

EXECUTIVE SUMMARY

In 1997 Congress recommended and funded a program to develop and demonstrate effective ways to secure military healthcare information systems. The Defense Healthcare Information Assurance Program (DHIAP) was developed in response to that recommendation with the purpose of identifying weaknesses in current medical information systems and developing prototype systems to provide reliable access to healthcare information while protecting it from unauthorized access or alteration.

The first step in accomplishing DHIAP's goal involved evaluating existing military medical information systems and their operational environments at military Medical Treatment Facility (MTF) sites; the DHIAP evaluation team identified vulnerabilities in the MTF information assurance capabilities and recommended operational procedures and policies to address those vulnerabilities. The second step was to study the technical vulnerabilities that were found for areas where application of technology could reduce or even resolve significant exposures. A review of alternatives with representatives of the MTFs that would serve as trial sites for the technology demonstration resulted in the decision to build a prototype that would provide Army-mandated compliance with the Remote Authentication Dial-In User Service (RADIUS) standard. This report provides the findings and conclusions of the effort to develop the technology and perform MTF trials of the RADIUS-compliant prototype.

The DHIAP Team worked closely with MTF technical representatives to confirm Army requirements relative to the RADIUS standard, then examined the marketplace for hardware and software components that met Army and RADIUS requirements and satisfied many of the "preferences" expressed by the MTFs participating in the effort. After building a prototype in a laboratory environment, the Team performed local and cross-facility trials. Finally, they implemented the prototype at the MTFs, tested it, built installation and operating procedures to guide early use of the system, and transitioned the technology to the sites for permanent use with their remote dial-in users.

The demonstration of DHIAP's prototype clearly showed the ease of implementing it in the Army's existing regional network environment, its ability to work within the regions' and sites' Windows NT-based technical environment, and, most importantly, its effectiveness in providing RADIUS compliance for remote dial-in users of military healthcare systems. The demonstration sites are continuing to use the prototype to control access by remote dial-in users even though the trials have ended; they are making plans to carry the technology forward with the necessary changes in their systems environments.

Section IV of this report provides high-level recommendations for program management and programmatics of a broader implementation of the DHIAP RADIUS-compliant prototype that will produce a timely, efficient implementation of the technology across Army MTF sites.

I. INTRODUCTION

DHIAP BACKGROUND

The United States Congress, the Secretary of the Army, and the Chief Information Officer of the U.S. Army Medical Command recognize that the current medical information systems are vulnerable to attacks on the availability, integrity, and confidentiality of their healthcare information. To address these issues, Congress recommended and funded a program to develop and demonstrate effective ways to secure military healthcare information systems.

In their normal operation, healthcare information systems create, store, access, transfer, and exchange sensitive but unclassified information. The challenge is to handle the information in such a way as to protect the privacy, confidentiality, and integrity of the data while still providing efficient and effective access to authorized users when and where needed. To meet this challenge and identify the most effective ways to integrate proper policies, procedures, methods, and technologies into existing military or healthcare information systems requires the following:

- An understanding of present, near term, and future policy and requirements for assuring the privacy of healthcare information;
- An understanding of the present state of the information security within the healthcare community;
- An analysis and documentation of functional requirements to improve requisite security while minimizing negative impact on required operational effectiveness; and
- A demonstration in the healthcare domain by installation and operation of a prototype to evaluate the effectiveness and operational impact of proposed security improvements.

The Defense Healthcare Information Assurance Program (DHIAP) was developed to meet the Congressional and Army goals. The purpose of DHIAP is to assess the present state of information security within the military healthcare system and to demonstrate prototype systems that provide reliable access to military healthcare information systems while protecting that information from unauthorized access or alteration.

One major effort in accomplishing the goals of Phase I of DHIAP involved evaluating the operational environments and medical information systems at military Medical Treatment Facilities (MTFs) against both expert knowledge of security practices that should be in place and current Army regulatory guidance for protection of patient information. The goals of this activity were to determine vulnerabilities in information assurance capabilities and recommend operational policies and procedures to address those vulnerabilities.¹ Known as DHIAP's Information Security Evaluation (ISE) effort, this activity culminated with publishing the *Phase I Composite Evaluation Report (ATI IPS TR 00-02)*. The report documents the results of the evaluation, outlines specific actions to address reported vulnerabilities, and provides

¹ **Appendix A** lists Army regulations and other publications used as references in this investigation. Note that the pending legislation and regulatory guidance of Health Insurance Portability and Accountability Act of 1996 (HIPAA), expected to be effective during 2000 and requiring compliance about two years afterwards, will further affect requirements for privacy of individually identifiable health information.

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

recommendations to management for improving information protection within the Army's medical organizations.

The other major effort of DHIAP Phase I used the ISE information as its starting point. This “Technology Demonstration” effort began by prioritizing the vulnerabilities relative to site priorities and determining candidate efforts where application of technology could demonstrate a significant reduction in (or resolution of) a significant exposure. A review of the alternatives with MTF staff that would be involved in the DHIAP technology development and demonstration effort confirmed MTFs’ need for authentication, authorization, and accounting/audit of their remote access capabilities and resulted in the decision to build a prototype technology to comply with the Army directive for Remote Authentication Dial-In User Service (RADIUS).² This *DHIAP Phase I Technology Demonstration Report* provides the background, findings, and results of the prototype demonstration effort, as well as recommendations for adapting the DHIAP prototype RADIUS-compliant implementation to be a cost-effective, manageable, and dependable solution for the Army’s multi-region medical processing environment.

PURPOSE OF REPORT

This report was compiled to provide MEDCOM and other military organizations with the design of DHIAP’s RADIUS-compliant system, an assessment of current-day operational realities that either aid or restrict its effectiveness, and recommendations for action.

REPORT ORGANIZATION

The following subjects are covered in this report:

II. Technology Demonstration reviews the DHIAP Phase I activities that produced the successful RADIUS-compliant DHIAP prototype. It outlines design requirements established by MTF needs and the Army and Internet Engineering Task Force standards for RADIUS compliance, summarizes activities that occurred during design and development of the DHIAP RADIUS prototype, and reviews major events of the technology trials and transition. Appendices A through D provide supporting detail for the material in this section.

III. Results and Observations assesses the capabilities of the DHIAP RADIUS-compliant prototype based on its performance during the system demonstration activity. After examining the prototype’s fit to the Army’s mandated and operational technical environment, it reviews the type of configuration that should be installed at various types of MTF sites and why. The section concludes with descriptions of the prototype’s ease of installation and its ease of operation and maintenance.

IV. RADIUS Implementation in the Army Medical Domain outlines the major programmatic considerations for a broad (e.g., regional) implementation of the DHIAP RADIUS-compliant technology. It describes the various options for equipment (and capability) distribution across multiple sites and provides high-level pros and cons for selection of each option. It provides information on programmatics of a RADIUS implementation, including cost analysis, project

² The DISC4 message is included as **Appendix B**.

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

planning, and resources. It concludes by providing some basic information on MTF-level considerations for staffing and training to support the technology.

Appendix A lists reference documents used by the Team to increase their understanding of the existing and planned military operations, policies, and procedures.

Appendix B is a copy of the HQ DA, DISC4, Washington DC message, subject: Network Security Improvement Program (NSIP) – Army Dial-in Standards and Policy, dtg 231300Z April 1999.

Appendix C is an excerpt from the Internet Engineering Task Force’s documentation of the RADIUS standard, outlining the purpose of RADIUS and what is meant by its Authentication, Authorization, and Accounting.

Appendix D is an overview of the DHIAP RADIUS-compliant prototype’s equipment configuration and its processing flows for RADIUS Authentication, Authorization, and Accounting.

Appendix E is a listing of the acronyms and abbreviations used in this report.

INTENDED AUDIENCE

This document is a report of a cost-effective, efficient approach to implementing RADIUS-compliant technology in the military MTF environment. There are multiple audiences for this information:

- Because the material could be equally applicable to the operation of any MTF, individual sites may be interested in this report as a resource for identifying and addressing a methodology for protecting its data during remote access by users.
- Because the material describes demonstration of a successful RADIUS implementation in a regional MTF and its subordinate community hospital, along with suggestions for making the tested implementation more flexible and dependable for a true “regional” implementation, higher echelons may use this report in defining a command-wide approach to implementing RADIUS compliance.

The DHIAP Team has provided the prototype design and recommendations for implementation, based on observations of the participants and the Team, to support Command action required for broad implementation of secure remote access by users.

II. TECHNOLOGY DEMONSTRATION

SUMMARY OF DHIAP PROGRAM ACTIVITIES

Phase I of DHIAP consisted of four major work activities, each designed to build on the results of preceding efforts. The first activity performed vulnerability research at selected Army Medical Treatment Facilities (MTFs); the remaining activities identified, developed, and tested a prototype technology to address one or more of the identified vulnerabilities. The activities and their work results are depicted in **Figure 1** and described below.

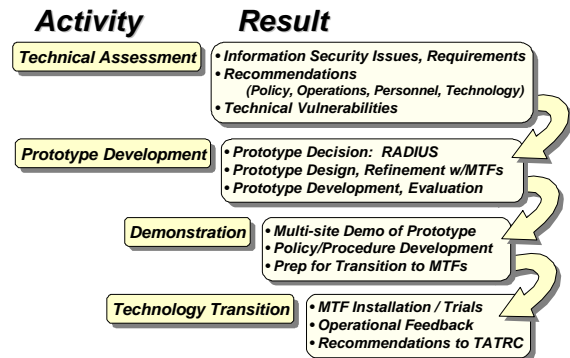


Figure 1 – Summary of DHIAP Phase I Activities

PROJECT PARTICIPANTS

The DHIAP RADIUS demonstration was conducted under the auspices of the Telemedicine and Advanced Technology Research Center (TATRC) of the Medical Research and Materiel Command (MRMC). The DHIAP Team of information protection, security, and healthcare experts included the following organizations:

- **ATI** (Advanced Technology Institute), Information Protection Technology Group
- **LMES** (Lockheed Martin Energy Systems), Data Systems Research Division
- **SEI** (Software Engineering Institute), Networked Systems Survivability Program
- **ADL** (Arthur D. Little, Inc.), Program Management Office
- **Government representatives** from TATRC/MRMC

The Army organizations that participated in the DHIAP RADIUS demonstration effort are:

- **Dwight David Eisenhower Army Medical Center (DDEAMC)** at Fort Gordon, Georgia
- **Winn Army Community Hospital (WACH)** at Fort Stewart, Georgia
- **Southeast Region Medical Command (SERMC)** at Ft. Gordon, Georgia

DDEAMC is the regional medical center for Army Medical Command's Southeast region. WACH is a community hospital within the region. SERMC has regional staff responsibility for medical operations, to include information processing among the region's facilities.

TECHNICAL ASSESSMENT

In this effort the DHIAP Team's experts in system security and healthcare facility administration performed onsite technical evaluations at two military MTFs to identify healthcare information security issues and requirements. In addition to generating recommendations for improvements in policy, operations/procedures, personnel/staffing, and technology, the Team's analysis of

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

findings provided specific insight into the sites' technical system vulnerabilities. Detailed technical recommendations were provided directly to the sites. A composite report of problem areas identified and recommendations for remedial action was provided to TATRC as *ATI IPS TR 00-02, DHIAP Composite Evaluation Report*. As a result of the technical evaluations of the MTF sites, the DHIAP Team was able to recommend candidate demonstration projects to improve certain aspects of MTF security.

PROTOTYPE DESIGN AND DEVELOPMENT

Prototype design and development consisted of working with the sites to analyze the technical and operational requirements for a demonstration system, investigate the various possible approaches to satisfying the requirements, present the options to the affected sites and to TATRC, install and demonstrate the capability in a laboratory environment, install, test, and configure the prototype capability at the sites, and transition the operational systems to the sites.

Selection of RADIUS as the DHIAP Demonstration Prototype

After a number of information protection vulnerabilities were identified during the Information Security Evaluations (ISEs) conducted earlier by the DHIAP Team at two military MTFs, the Team prioritized these vulnerabilities, using criteria shown in **Figure 2**. Prioritization was also influenced by the Team's opinion of how best to make a difference in information security at the MTF. Armed with knowledge of the high priority vulnerabilities, the team performed research to identify technology development efforts that would address them. Finally, they returned to sites that had participated in the ISEs to conduct working sessions and targeted analyses with the sites' technical staffs to ensure that they had identified all relevant technical and operational issues.

- Relevance to MTF needs
- Relevance to TATRC mission
- MTF authority to direct and implement change
- Cost
- Complexity
- Existence of a technical solution

Figure 2 – Criteria for Prioritizing Information

The Team's initial technology proposal to the MTFs was to implement secure e-mail service using secure socket layer (SSL) sessions in order to protect information in transit between the remote users and the MTF computing environment. MTF staff responded that they had already begun to implement SSL for electronic mail, but needed technical assistance to comply with the Army directive for implementing the Remote Authentication Dial-In User Service (RADIUS).³ Their goal in implementing this capability was to provide the site with much improved identification and authorization of the remote users who access hospital systems via dial-in.

MTF staff, TATRC, and the DHIAP Team agreed that DHIAP's Prototype Demonstration would implement a RADIUS-compliant server capability fulfilling the Army's requirement for identification and authentication of dial-in users. As an important extension to the RADIUS demonstration, they arranged for the implementation to involve both a regional medical center and an associated community-level MTF and for testing and trials of the technology to include both local and cross-facility communications.

³ HQ DA, DISC4, Washington DC message, subject: Network Security Improvement Program (NSIP) - Army Dial-in Standards and Policy, dtg 231300Z April 1999; the message is included as **Appendix B**.

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

Prototype Design

Design of the DHIAP prototype technology began with documenting technical security requirements outlined in the Army's RADIUS guidance. Requirements outlined in the Internet Engineering Task Force (IETF) specification of the RADIUS standard⁴ added some detail to the design, and the operational requirements and preferences noted during the technical research with trial site MTFs further enhanced the documentation. **Figure 3** summarizes the Army's requirements for RADIUS implementation, along with requirements added by the MTFs that would be testbeds for the DHIAP prototype demonstration. The MTFs' core selection criteria included compatibility with the MTFs' existing systems, support for browser-based administration, support for remote auditing, and minimizing the MTFs' cost of follow-on support. It was also important that the selected technology support growth in the number of lines and types of communications.

Armed with an understanding of requirements, the Team searched the marketplace for compliant components. Their resources included the Internet, technical journals, contact with vendors, and discussions with personal contacts that the Team members considered experts in the router and computer security industry. The alternatives considered are listed in **Figure 4**.

Based on evaluation of the capabilities of the compliant components, knowledge of the technical skills available within the MTFs' Information Management Divisions, awareness of components already in place at the MTFs, and their own personal experience in using many of the candidate tools, the Team recommended that the technical solution for the RADIUS prototype be the Cisco 3600 series router with an Intel-based computer running Windows NT Server and CiscoSecure software.

Prototype Development and Evaluation

DHIAP prototype systems were initially installed at Lockheed Martin Energy Systems in Oak Ridge TN and the Advanced Technology Institute in North Charleston SC. These laboratory installations highlighted situations that were likely to arise later during installation at MTFs. In addition, they gave the system developers and component vendors the opportunity to test all the system options and to make configuration recommendations prior to installing the systems in an

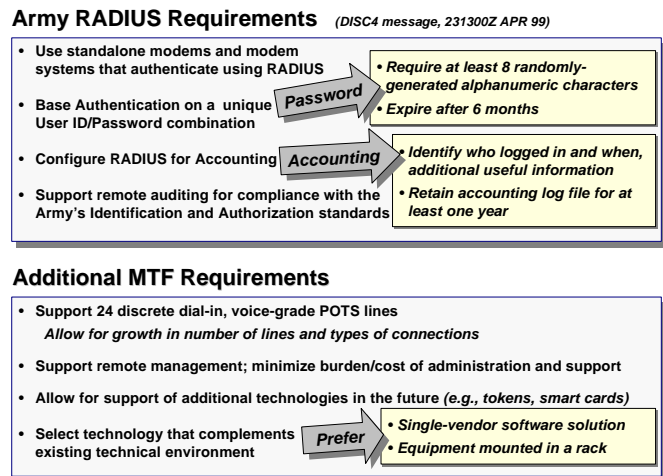


Figure 3 – Army and MTF Requirements for the DHIAP Prototype

- ☒ VOP RADIUS Server -- Vircom Products
- ☒ Total Control Access Platform -- 3COM
- ☒ Remote Authentication Dial-In User Services -- Bay Networks
- ☒ MiniArray III -- MultiTech Systems
- ☒ PortMaster -- Lucent Technologies
- ☒ Remote Access Server -- Microsoft
- ☒ CiscoSecure -- CISCO Systems

Figure 4 – Technology Alternatives Reviewed by the DHIAP Team

⁴ Appendix C contains an overview of the IETF RADIUS standard.

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

operational environment. The laboratory testing provided the opportunity to evaluate the suitability of the system relative to design requirements. Concurrent with the installation and testing period, the prototype design and configuration recommendations were informally evaluated by individuals from the Software Engineering Institute for fit to the stated requirements and for the impact on enhanced security. The proposed prototype was considered to meet the functional requirements as stated. Specifics of the design and processing of the prototype are provided in **Appendix D**.

DEMONSTRATION

The Team's evaluation of the RADIUS capabilities in the multi-site lab environment showed connection of a dial-in user through a RADIUS prototype configuration consisting of both a UNIX system emulating a CHCS Telnet connection and a Web Server/NT Server configured to represent an MTF's Exchange Web Server. The DHIAP Team's demonstration of this capability to an audience that included TATRC program managers and the technical staff from the test sites resulted in a validation and verification of the prototype's capabilities for authentication, authorization, and accounting of remote access dial-in users. The successful laboratory demonstration provided the sites with an understanding of equipment capabilities and led to their agreement to install an Initial Operational Capability (IOC) at their sites.

The systems were installed at the identified test sites shortly after completion of the lab demonstration, and the MTFs were given an IOC to provide an opportunity to become familiar with system operation, plan for operational procedures, and plan for the migration of their user population to the new capability.

TECHNOLOGY TRANSITION

Following installation, the DHIAP Team trained MTF staff on the installation, configuration, operation, and maintenance of the system. In addition, the Team reviewed the sites' policy and procedures for support of secure system operations. The MTF sites operated the RADIUS-compliant systems, configured their remote dial-in users, produced user guidance, and monitored the remote users' activity in accessing MTF systems. Full Operational Capability (FOC) was scheduled for approximately 30 to 45 days following the IOC.

Soon after implementation, the sites were able to transition the DHIAP RADIUS-compliant system from testing to full operational status. MTF staff enhanced their operational procedures and documentation while the DHIAP Team used the MTFs' feedback on their operational experience with the technology as the basis of their recommendations for the Army's future enhancement of the DHIAP RADIUS prototype and its related policies and procedures.

III. RESULTS AND OBSERVATIONS

The architecture and components of the prototype developed for trials at DDEAMC and WACH, the Army MTFs participating in the DHIAP RADIUS demonstration, are suitable for use in other MTFs. The DHIAP prototype meets the Army requirements for modem dial-in standards and policy (see **Appendix B**), in which the RADIUS standard was selected as the required method for implementing authentication, authorization and accounting. **Table 1** below provides a comparison of the Army requirement for a dial-in system (based on the Army message and the RADIUS standard) and summarizes the DHIAP prototype's satisfaction of these requirements. The DHIAP prototype provides flexibility for Army facilities while supporting the Army's requirements for RADIUS-compliant systems.

Table 1 – Army Dial-in User Requirements vs. DHIAP RADIUS System

Army Requirements for Dial-in Users⁵	DHIAP RADIUS System Implemented
Standalone modems and modem systems with dial-back capability that authenticate using RADIUS are the only allowable modems.	DHIAP prototype implementation adheres to the RADIUS standard. It is a site implementation responsibility to assure that all modems go through RADIUS.
Dial-in operations will be authenticated with a unique user-id and password.	User IDs and Passwords are unique and may be stored on either the AAA Server or the region's NT User Database.
Passwords shall be at least eight randomly generated alphanumeric characters.	Minimum password length is selectable on both the AAA server and the region's NT Primary Domain Controller.
Passwords shall be passed in encrypted format.	Passwords are sent between NAS and AAA Server in encrypted format.
Passwords shall reflect the current Army password expiration policy of 6 months.	Password expiration time is selectable on both the AAA Server and the region's NT Primary Domain Controller.
RADIUS software shall be configured for accounting.	Multiple accounting logs, configurable by the system administrator, are maintained.
Accounting logs will show, at a minimum, who logged in and when; log files will be retained for a year.	Accounting information includes User ID, session start date and time, session end date and time, user IP address, NAS port, and failed logins; system configuration changes are also logged. The system administrator determines the schedule for log file backup and archiving; logs may be backed up to either a central repository on the network or a dedicated tape. It is a site responsibility to store logs for at least a year.
Servers will be remotely audited to ensure all standards established for Army Identification and Authorization are met.	A browser interface provides remote access to log files; remote privileges are configurable.

The DHIAP RADIUS-compliant prototype is designed to meet RADIUS standards, assuring that the remote dial-in users who request access to the MTF network and other military network resources: (1) are who they claim to be, and (2) obtain access only to resources approved for their use by dial-in. Access by the remote user is logged to a RADIUS-compliant accounting log.

In addition to Army requirements, the information systems groups at the MTFs and regional levels have their own "local" preferences for hardware/software features and capabilities. Two important factors about the MTF environment are that information technology staff at MTF and region levels have limited administrative resources and there is a need for future expansion of capabilities of the RADIUS-compliant system. The configuration selected by DHIAP for the

⁵ Summarized from Army HQ DA message, dated 23 April 1999 (see **Appendix B**)

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

RADIUS-compliant system will support the local requests by providing the additional features summarized in **Table 2**.

Table 2 – MTF-Requested Features of the DHIAP RADIUS-Compliant System

Type	Feature
System Administration	<ul style="list-style-type: none">• Maintenance overhead is reduced by use of hardware and software common in SERMC: Windows NT Server software, CISCO Router, and Cisco IOS software• Administrative burden is reduced by authenticating users against SERMC's existing Windows NT Domain Name/Password database• Local and remote network administration are supported by the browser interface
Flexibility / Extensibility	<ul style="list-style-type: none">• Support for the expansion of security features through use of third-party token-card servers (SecurID, Enigma Logic, SecureNet, and any hexadecimal X.909 devices)• Support for time-of-day access control, providing day, time and duration control• Support for 10BaseT and 100BaseT network connections• Scalable implementations to support clinic, hospital and region locations• Support for interconnected multi-site implementations• Support for minimum configurations at smaller sites• Support for redundancy through network connectivity

These features minimize the amount of additional hardware and software training required to support the RADIUS-compliant system without limiting the technology's expansion and scalability.

MINIMUM CONFIGURATION

The DHIAP prototype configurations installed at each of the two trial sites included full capabilities in order to allow thorough testing, initially as standalone systems and then as cooperating systems on a network. In the prototype configuration, the AAA Server manages the RADIUS authentication functions, while the NAS provides connectivity for the remote dial-in user and manages the user's access to authorized resources. A NAS may be co-located with the AAA Server that performs its authentication or it may instead rely on a remotely located AAA Server for this service. (See **Appendix D** for a complete description of AAA Server and NAS processing.)

A "regional" implementation for three or more MTFs could take a different approach from that used in the DHIAP demonstration. That is, an economical regional implementation would place a complete configuration (AAA Server and NAS) at a limited number of locations and minimal configurations (NAS-only) at all other sites. In this scenario, the complete configurations remotely support the sites that have minimal configurations. This concept is discussed further in Section IV, "RADIUS Implementation in the Army Medical Domain."

The hardware and software used in the DHIAP demonstration was illustrated and their processing described in **Appendix D**; the same components are listed in **Table 3** below in the "Demonstration Prototype / Complete System" column. **Table 3** indicates differences in the equipment installed at "complete" vs. "remote" sites, and provides in the "Comments" column relevant information about the flexibility of the component or its features.

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

Table 3 – DHIAP RADIUS Hardware/Software Components

System	Demonstration Prototype / DHIAP Complete System <i>AAA Server and NAS</i>	Remote Site <i>NAS-Only</i>	Comments
AAA Server	Intel-based PC with 500 MHz processor, 128 MB memory ⁶	NONE	<ul style="list-style-type: none">PC processor and memory affect the processing time required to resolve authentication requestsBecause the PC's workload (which is limited to authentication/logging activities only) is light, DHIAP implemented NT Server software on workstation hardware instead of the more expensive server hardware
	<ul style="list-style-type: none">20 GB hard drive (or greater)		Disk size requirement varies with amount of logging (i.e., number of concurrent dial-ins) and frequency of log archiving
	<ul style="list-style-type: none">12/24 GB DAT (tape) drive (or greater)		DAT is used for hard drive backup; note that local procedure to back up to existing Network Archives may replace need for tape
	Windows NT Server software		
	CiscoSecure software		
NAS	Cisco 3640 router <ul style="list-style-type: none">Analog modem bank (56 KB modems in groups)Other features: 10/100 MB Ethernet card, 16 MB non-volatile memory Cisco IOS software	SAME	<ul style="list-style-type: none">Modem banks include 8, 16, 24, or 32 modemsMore than 32 modems may be provided by installing multiple NAS Servers at a siteInterface cards for ISDN and T1 dial-in lines may also be used in the NAS with a corresponding reduction in the number of available modem banks
UPS	1400 VA	SAME	If AAA and NAS are attached to a pre-existing source of uninterruptible power, UPS is unnecessary

EASE OF INSTALLATION

Implementing the DHIAP technology is a matter of installing and configuring its commercial off-the-shelf tools. As with all technology installation, staff members' ability to apply related experience generally reduces the time and complexity of the task. By selecting components that were closely related to the products already installed in the MTFs, the DHIAP Team was able to take advantage of the MTF Information Management staffs' existing technical expertise.

The learning curve for installing and configuring the DHIAP RADIUS-compliant system is greatly reduced when the system administrator has prior experience with the Windows NT Server and Cisco IOS operating systems. This knowledge, used in conjunction with the *DHIAP RADIUS Supplemental Installation and Maintenance Guide (ATI Special Report IPS 00-03)* and applicable vendor documentation, should lead to a straightforward installation. A system administrator who has successfully installed one DHIAP RADIUS-compliant system should require minimal additional knowledge to install systems at additional sites. An administrator with no experience in Windows NT or Cisco IOS software will require outside assistance from the vendors or other experts.

⁶ Other features of the PC include: CD-ROM drive, 3.5 diskette drive, Ethernet card, keyboard, mouse, and 17" monitor

EASE OF OPERATION AND MAINTENANCE

Support for Remote System Users

A remote user's computer (home, laptop, etc.) must be configured as a dial-in client before it can be used for remote access to MTF systems. The configuration is a straightforward process; detailed procedures for configuring Windows 95, 98, and NT dial-in clients are included in the *DHIAP RADIUS Supplemental Installation and Maintenance Guide (ATI Special Report IPS 00-03)* or in Microsoft documentation. Once the user's client machine has been configured, there should be little or no need for change.

From the point of view of the remote user, dial-in processes and procedures under the RADIUS-compliant approach are similar to methods used previously. Once the dial-in connection is established, the user's view and operation of the accessed systems is similar to operation at the work location. One important difference to the user is that access to particular systems used locally may be denied when dialing in from a remote location. For example, user access to a system such as CHCS might be necessary for day-to-day work in a nursing unit but inappropriate for access from home.

Support of User Accounts

Administration of user accounts (i.e., the User IDs and Passwords) requires minimal effort when, as occurs in SERMC's DHIAP implementation, AAA Server user authentication is performed against the NT User Database on the region's NT Domain Controller. In addition to holding the user's User ID and Password, the NT User Database holds an indicator of whether the user should be allowed to access the network remotely; if the NT indicator is set to deny remote access, the user will fail the RADIUS authentication process and network access will be denied.

Figure 5 depicts relationships among the system resources involved in the DHIAP authentication that is based on the region's NT User ID/Password structure. To obtain access to system resources, a user must either have been predefined in the AAA Server's User Database⁷ or have been authenticated against the NT User Database as an NT user who is allowed remote access. As described previously, authenticated remote users are given the type of access dictated by the User Group entry in the AAA Server's User Database entry (the "reference to user entries in NAS ACL"). If no AAA entry exists for the remote user, the RADIUS-compliant system temporarily assigns the user to a "default" User Group that permits limited forms of access.

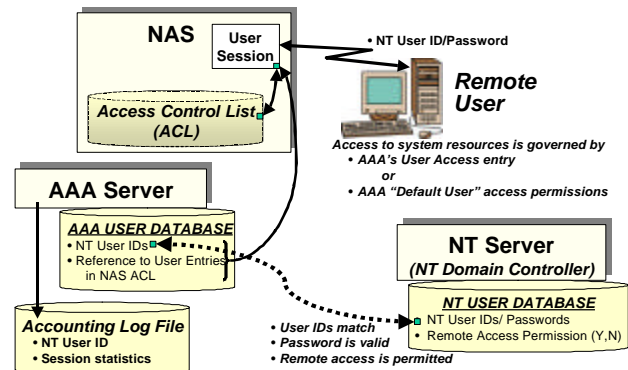


Figure 5 – DHIAP's Use of Region's NT Structure

⁷ Although procedure calls for all of a region's User IDs/Passwords to be maintained on its NT User Database, it is possible (but not recommended) for the system administrator to record a User ID/Password directly on the AAA Server's User Database. This might be done as a temporary measure (e.g., to permit short-term network access for a known and approved non-NT user).

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

Upon receiving appropriate instruction, a system administrator can move the user to a predefined User Group that permits the type of access that is more appropriate to the user's role at the facility. (Note that most types of access permitted at a site can typically be provided with a relatively small number of CiscoSecure user groups.) **Figure 6** provides an example of the types of access permissions that might be made available to different types of users at a facility. In this scheme, individuals with an "office worker" type of job might be assigned to a User Group that allows e-mail and Internet access, while a "physician" might be in another group that allows e-mail, Internet, and CHCS access.

GROUP #	MTF ROLE	ACCESS PRIVILEGES
Default	Undefined or Uncategorized NT Users	E-mail
10	System Administrators	All systems and privileges available on their office computers
20	Medical Staff	E-mail, Internet, and CHCS
30	Staff	E-mail and Internet
40	Command Staff	All systems available on their office computers (e.g., E-mail, CHCS, network files)

Figure 6 - Typical Group Privileges for an MTF

Categorization of individuals into access groups eases the burden placed on system administrators and improves accuracy when working with a large number of users.

System administrators use a CiscoSecure browser-based interface to add, change, and delete user access permissions; the design of the interface makes this maintenance an efficient process. Once a particular group's access rights have been defined, assigning existing users to the group is accomplished by associating the user with the appropriate group. Each user inherits the privileges allowed for the group; there is no need to create and maintain separate privilege lists for each individual remote user.

Support of Accounting Logs

The system administrator's work with the CiscoSecure Accounting Log function begins with defining the information to be logged. The system administrator uses the CiscoSecure browser interface to modify both the types of logs that are maintained and the type of information logged. Ongoing, the system administrator monitors the logging activity, works as needed with the information captured on the logs, and regularly archives (or backs up) the log files.

In monitoring the logs, the system administrator should regularly review the captured information to identify unusual circumstances and initiate appropriate action. As with log maintenance, the monitoring of accounting logs is performed using the browser-based interface. Certain log monitoring activities may be automated: the system administrator may customize CiscoSecure to send an electronic alert when a particular type of activity occurs (e.g., excessive login attempts). CiscoSecure will then generate an alert via e-mail or pager to predefined destinations as timely notification that the questionable event has occurred.

Accounting logs must be periodically archived to backup storage media. Frequency of archiving is based on site preference, typically associated with the file's size relative to space available. Log retention, set by the system administrator using CiscoSecure's browser, may be based on time or file size, or may be left under manual control. The method of archiving is also a site-dependent decision: one approach is to archive the logs as part of regular network backups at the site, another is to archive to tape (a tape drive is included in the DHIAP complete system's configuration for this purpose).

IV. RADIUS IMPLEMENTATION IN THE ARMY MEDICAL DOMAIN

Implementing effective solutions for securing military healthcare information systems is one of the primary objectives of DHIAP. DHIAP's investigations of information protection vulnerabilities at representative regional and community hospital MTFs,⁸ and its demonstration of a prototype technology for authenticating and authorizing remote system users, can provide useful direction and tools for Army MTFs.

DHIAP's RADIUS-compliant prototype was designed for simple insertion at the point of dial-in access of an existing network structure. It was demonstrated in SERMC where the network structure is based on Windows NT 4 and system users are defined within the region NT system's Domain Controller. Like all Army medical facilities, SERMC is part of MEDNET's regional and command-wide communications infrastructure. Since the other Army medical regions use a similar pattern of centralized control over user access permissions, it is likely that implementation of the DHIAP RADIUS-compliant prototype would be straightforward throughout MEDCOM.

It is important that a broad implementation of the DHIAP RADIUS-compliant technology (i.e., multi-region or command-wide) be planned and overseen by a central coordinating authority. As outlined in this section, critical subjects such as technical approach, project planning, equipment configuration and acquisition, procedures, and operational staffing are handled more economically and efficiently by the distributed implementation teams when guidelines have been provided by a central authority. Project oversight by the same authority would assure that coordinated efforts proceed according to a plan.

For simplicity and clarity, the following analysis and recommendations are based on a MEDCOM implementation. It is recognized that the central coordinating authority may be a function of the Army or DISA communication planners, but it may also be a function of the medical Tri-Service Infrastructure Management Program Office (TIMPO). Rather than attempt to sort out the chain of responsibility in the DoD, this report contains generic recommendations equally applicable to any office assigned responsibility.

TECHNICAL APPROACH

The network infrastructure of the Army MTFs is integrated by the Army's regional medical network, MEDNET. MEDNET provides high quality communication links among the MTFs, Army command, and the Internet. DHIAP's RADIUS-compliant system can use MEDNET facilities to safely integrate multiple RADIUS-compliant systems by capitalizing on the existing high bandwidth network connections and the regional NT domain architecture and imposing only a slight additional load on the wide area network.

This section outlines three technical approaches to implementing DHIAP RADIUS compliance throughout a region. The first approach makes each site autonomous by installing a complete DHIAP prototype configuration. The second places a complete DHIAP prototype configuration at one site (assumed to be the location of region headquarters) and has all other sites in the region communicate with the central regional site for their authentication, authorization, and accounting services. The third option is similar to the second, except that it adds a second (i.e., redundant)

⁸ For a detailed summary of findings, refer to *ATI IPS TR 00-02, DHIAP Phase I Composite Evaluation Report*.

complete configuration at one of the region sites to serve as backup in case of problems with the region's AAA Server (the component that authenticates the remote user). Each option offers advantages and disadvantages, reinforcing the importance of having a higher echelon authority determine the coordinated technical approach to be followed in a broad implementation. **Appendix D** provides a technical overview of the DHIAP equipment configuration and the major processing steps that occur during the Authentication, Authorization, and Accounting of the DHIAP RADIUS-compliant process. Operational capabilities offered by the three options are summarized in the sections that follow.

Autonomous Complete RADIUS-Compliant Systems at Every Site

The most direct implementation option in a region is to place a complete RADIUS-compliant system (consisting of AAA Server and NAS) at each MTF site, as depicted in **Figure 7**. (This is the approach used for trial site testing of the DHIAP prototype.) The solid black line in **Figure 7** indicates that each site's authentication is performed locally; the dotted line indicates the authenticated user's access to network resources. The demonstration configuration shown in **Figure 7** does not take full advantage of the system's capabilities (e.g., it offers no backup in the case of hardware or software problems in the AAA Server or NAS). Benefits of the configuration are that all Authentication / Authorization / Accounting communications are local to the site, with no reliance or additional traffic placed on the MEDNET. This approach utilizes MEDNET only for authorized user communication with resources at distant sites.

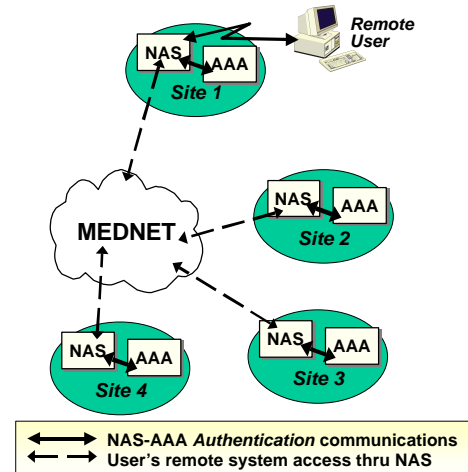


Figure 7 - Autonomous Configuration – Complete Systems at All Sites

Complete System at Central Site and NAS at All Satellite Sites

A second option for regional implementation is to install a complete RADIUS-compliant system (NAS and AAA Server) at one site (e.g., at the region headquarters location) and put NAS-only at all other locations in the region (e.g., MTF and clinics with dial-in users). Here, each remote NAS interacts with the AAA Server at the Region via the MEDNET. **Figure 8** depicts the equipment and connectivity in this option; the solid black line in the diagram indicates the processing path for authenticating a dial-in user, and the dotted line indicates the path for user access to network resources. The difference between this processing and that depicted in **Figure 7** is that a NAS is physically located at one site while its AAA Server is at a geographically distant site.

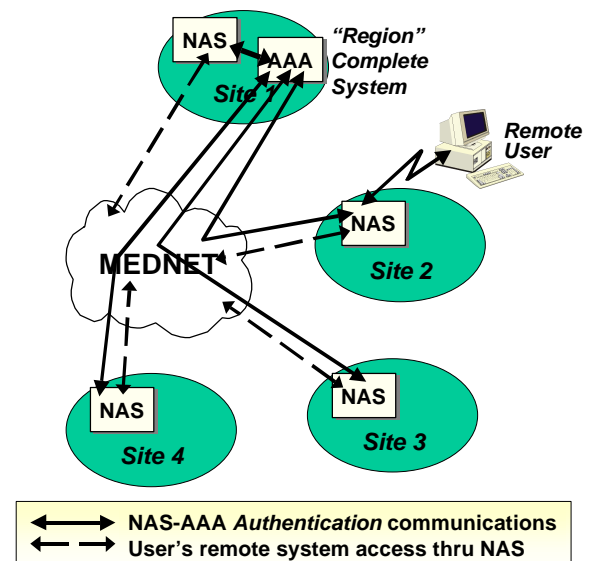


Figure 8 - Central Configuration – Complete System at One Site and NAS-Only at Remaining Sites

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

Due to the minimal amount of information passed between NAS and AAA Server (the User ID and encrypted password in a 120-byte package, and a 155-byte acknowledgement consisting of either the User ID and the authorized ACL or the User ID a denial indicator), servicing this client-server relationship via the T1-speed MEDNET is feasible. Based on the current bandwidth of the MEDNET backbone, the amount of AAA traffic across the system will have a minimal effect. This option reduces installation cost since only the cost of NAS is borne for the remote sites. In addition, it reduces the cost of system administration by centralizing most system maintenance and administrative responsibilities and integrating the administration work with maintenance and operation of the existing NT Domain Controller systems at the central location.

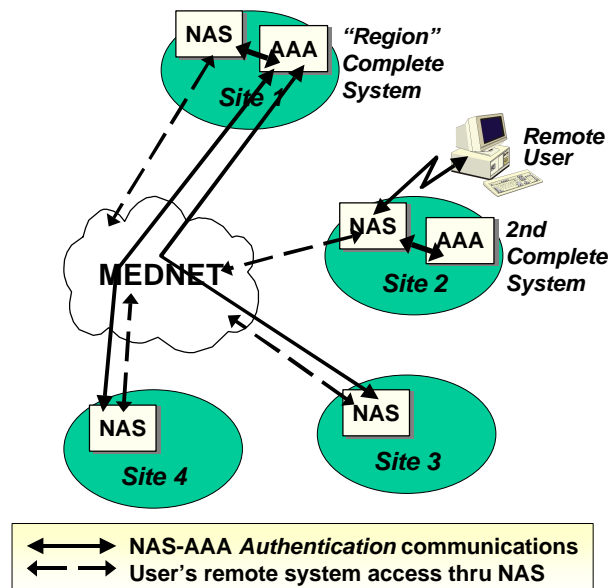


Figure 9 - Redundant Configuration – Complete System at Two Sites, NAS-Only at Remaining Sites

Redundant Complete Systems and NAS at Remaining Satellite Sites

A third option for regional implementation is to install a complete RADIUS-compliant system (NAS and AAA Server) at the region, install one or more additional complete systems at MTFs in the region, and install a NAS at the each of the remaining sites in the region. All systems are connected to MEDNET, allowing them to take advantage of system redundancy.

Figure 9 depicts the equipment, connectivity, and data flow for this option when all elements of the configuration are working properly. Figure 10 depicts operation when the primary AAA server fails. Because of the redundancy of complete systems, AAA access for the entire region can be switched from the region AAA Server to the "2nd Site" AAA Server. Note also that the region's NAS switches to the 2nd Site NT Domain Controller for authentication of its users. The redundant configuration option reduces cost compared to the first option (autonomous sites) by installing the minimum number of complete systems and using NAS at the rest. The complete sites can be administered by the

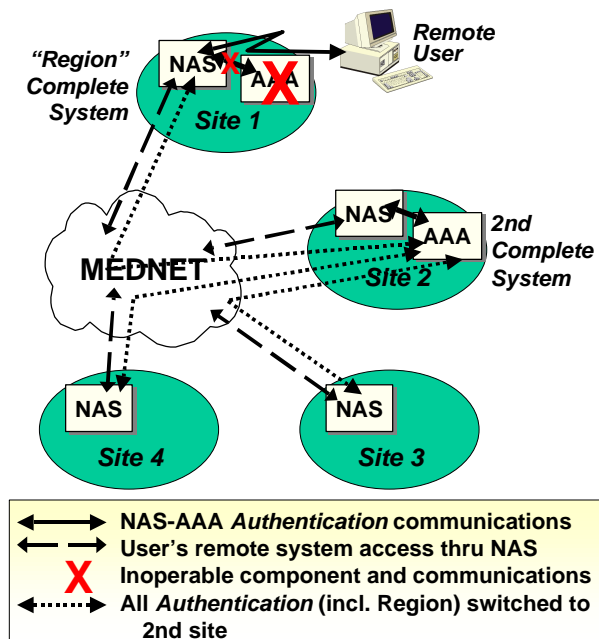


Figure 10 – Authentication by 2nd Site AAA Server When Primary AAA Server is Not Functioning

region, or locally, or both.

Note on Consequences of a Non-Functional NAS

Figure 11 illustrates that loss of a NAS means loss of dial-in service for the users who rely on that NAS. Unless its users have been provided with the capability of dialing to an alternate NAS under these circumstances, the downed NAS' users are prevented from accessing network resources until the failed NAS has been brought back online. Note that a user who knows the dial-in number for a different NAS in the region is able to connect and use network resources with no other change to the dial-in procedure.

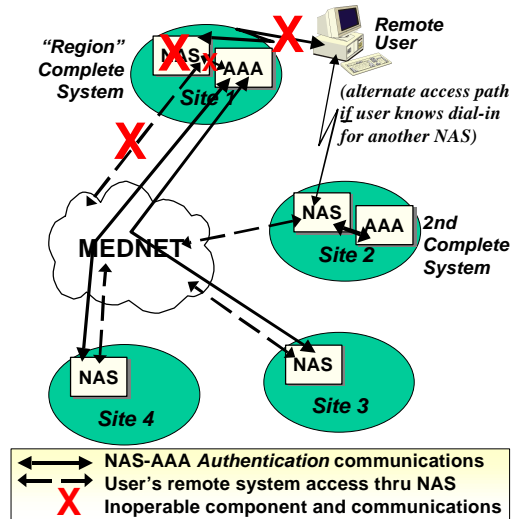


Figure 11 – Loss of Service to Users When Site NAS is Down

PROGRAM MANAGEMENT AND PROGRAMMATICS

A central command authority should commit to using a coordinated approach for MEDCOM's RADIUS implementation. Guidance on how such a project will proceed should include:

- Analysis of costs (which may lead to revising the technology approach),
- Guidance on how regions/sites are to fund the implementation costs,
- Development of requirements and guidance for project implementation by the region and MTF-level staffs,
- Definition of policy and general procedures for use of the implemented system,
- Establishment of project oversight capabilities (e.g., a project manager) to track overall progress and deal with issues as they arise, and
- Assignment of responsibility for providing technical guidance and training to sites on installing and maintaining the system.

While there are many issues requiring resolution in the above listing, this section of this report will provide information useful for planning for funding, training, policy, and technical guidance.

Cost Analysis

The funding required to implement the RADIUS-compliant technology varies with the approach selected and the number of sites to be installed. As described previously, the configuration for a region can vary from *autonomous* (a complete system installed at every site), to *centralized* (authentication/authorization performed at one site) and *redundant* (the centralized option with a second complete system available to assume control if problems are encountered at the central site). Sample costs of these configuration options are provided in **Table 4**. Each configuration shown follows an assumption that there ten sites in a region; activity at the Region site requires availability of twenty-four modems, five sites require availability of sixteen modems, and three small sites require the minimum number of modems (i.e., eight).

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

Table 4 -- Sample Costs for DHIAP Technology Options

Component ▪ Size Options		<i>Autonomous AAA</i>	<i>Central AAA</i>	<i>Redundant AAAs</i>
		AAA/NAS at All 10 Sites ⁹	AAA/NAS at Region + NAS-Only at 9 Sites ⁹	AAA/NAS at Region and 2nd Large Site + NAS-Only at 8 Sites ⁹
AAA	Intel-based PC with 500 MHz processor, 128 MB memory ¹⁰	2,850 * 10 (<i>All Sites</i>)	2,850 * 1 (<i>Region</i>)	2,850 * 2 (<i>Region</i> +2 nd <i>Site</i>)
	Windows NT Server 4.0 software including Service Pack 5.0	800 * 10 (<i>All Sites</i>)	800 * 1 (<i>Region</i>)	800 * 2 (<i>Region</i> +2 nd <i>Site</i>)
	CiscoSecure ACS 2.4 software	3,105 * 10 (<i>All Sites</i>)	3,105 * 1 (<i>Region</i>)	3,105 * 2 (<i>Region</i> +2 nd <i>Site</i>)
NAS	Cisco 3640 Router with <i>one of the following</i> :			
	▪ 24 modem ports – 56KB ¹¹	12,308 * 1 (<i>Region</i>)	12,308 * 1 (<i>Region</i>)	12,308 * 1 (<i>Region</i>)
	▪ 16 modem ports – 56KB ¹¹	10,812 * 6 (<i>6 Sites</i>)	10,812 * 6 (<i>6 Sites</i>)	10,812 * 6 (<i>2nd Site</i> + 5 <i>Sites</i>)
	▪ 8 modem ports – 56KB ¹¹	8,228 * 3 (<i>3 Sites</i>)	8,228 * 3 (<i>3 Sites</i>)	8,228 * 3 (<i>3 Sites</i>)
Other Equip	1400VA UPS	700 * 10 (<i>All Sites</i>)	700 * 10 (<i>All Sites</i>)	700 * 10 (<i>All Sites</i>)
	Open-sided Hardware Rack	900 * 10 (<i>All Sites</i>)	900 * 10 (<i>All Sites</i>)	900 * 10 (<i>All Sites</i>)
Ann \$	First-year Annual Maintenance for CiscoSecure ACS software ¹²	1,520 * 10 (<i>All Sites</i>)	1,520 * 1 (<i>Region</i>)	1,520 * 2 (<i>Region</i> +2 nd <i>Site</i>)
Ann \$	First-year Annual Maintenance for Cisco 3640 ¹²	0	950 * 9 (<i>9 NAS Sites</i>)	950 * 8 (<i>8 NAS Sites</i>)
CONFIGURATION COST for a “REGION”¹³		\$200,614	\$134,689	\$142,014

The costs shown in the table are in general alignment with the amount of capability provided. In the scenario shown, note that the *autonomous* configuration carries a 30% higher cost than the other options, and that the *redundant* configuration, which offers continuity of service, is only slightly more expensive than the *central* option.

Planning for Region- and MTF-level Projects

Program management should outline project requirements for the distributed organizations that will actually perform the implementation of RADIUS-compliant technology. This includes:

- A **briefing** for region- and MTF-level command to outline the purpose of the effort and initiate activity at the region and site level

The briefing should provide background on RADIUS compliance, funding, hardware/software being acquired, resource requirements for the effort, suspense dates, etc.

- A **generalized project plan** for region- and site-level general approaches to implementing the RADIUS technology.

The generic plan can be used as implementation guidance by regions and sites. By outlining the project's sequence of activities, estimated timeframes for completing each major activity, and types of staff/responsibilities of the MTF personnel who must

⁹ The equipment features and costs listed in **Table 4** were effective in March 2000. This summary is provided for general information only. The Army's actual cost analysis and acquisition decisions should be based on configuration requirements, product features, and costs as of the date of configuration analysis and acquisition.

¹⁰ and 20 GB hard drive, 12/24 GB DAT (tape) drive, CD-ROM drive, 3.5 diskette drive, Ethernet card, keyboard, mouse, 17" monitor

¹¹ and 10/100 MB Ethernet card, 16 MB non-volatile memory, Cisco IOS software

¹² Maintenance is a recurring cost for each year of operation

¹³ One-time and ongoing costs of communications services is not included

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

participate in the effort, it would provide the operational units with a single, consistent approach to performing their implementations. In addition, the plan can serve as a management tool for overseeing progress of the distributed efforts.

- **Training and policy documentation** to be incorporated into region- and site-level training on RADIUS and the Army's selected technical approach

Training material should provide a starter set of materials that each facility can use to train its management, technical staff, and users on the purpose and use of the RADIUS implementation. Central development of the initial package will allow training to be consistent across sites and will save development time that would otherwise be expended at every affected facility. Excerpts from this report and the *DHIAP RADIUS Supplemental Installation and Maintenance Guide (ATI Special Report IPS 00-03)* should be considered as resources for this effort.

Policy and Draft Operational Procedures

Implementation of the RADIUS-compliant technology advances the Army's security capability in several areas. In addition to the advances in user identification, limitation on remote user access to systems, and accountability that are the specific objective of a RADIUS implementation, the implementation will also provide incentive for sites to examine and revise their existing security policies and procedures. In mandating RADIUS compliance, the higher command authority should provide policy guidance sufficient for the sites to properly implement this improved security. Providing sample procedural documentation with the policy guidance will ensure that each site's procedures conform across a region and throughout the Army. Subjects of sample procedure are likely to include: the methodology for users to request remote system access (including the specific systems to be accessed); region-wide technical procedure for keeping RADIUS user access tables synchronized with the region's master database of user access permissions; technical procedure for maintaining the site's and user's remote access systems, etc.

Program Oversight and Technical Guidance

A designated program manager should be assigned responsibility for MEDCOM's RADIUS implementation

Since the implementation of RADIUS-compliant technologies is a technical endeavor, it is likely that the Army's region and site MTF staff may experience some technical challenges (as occurred with the DHIAP trial sites). Technical issues will also arise from the rapid pace of change in the technologies required for a RADIUS-compliant system. A central source of knowledge, with ability to perform specific research efforts and distribute the results to address a problem, will be a useful resource for all MEDCOM implementation teams. An added benefit is the Army's ability to learn from the questions being asked and implement a program of notices or training enhancements on subjects of widely experienced problems.

To provide an appropriate level of control over the effort, and to be effective in intervening when there are difficulties or delays, the following actions are recommended:

- Appoint a project manager with sufficient authority to track progress and deal with issues as they arise, and
- Create a center of expertise responsible for providing technical guidance to sites on installing and maintaining the system.

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

The experience gained by DHIAP demonstration sites should be a resource for any technology center formed for this program.

Site Considerations for Implementation

The predominant effect of a site's implementation of the DHIAP-developed RADIUS-compliant system on an MTF site will be to its remote system users and certain members of its Information Management Division (IMD) staff.

- The site's remote system users are affected in two ways. First, they must configure their remote computers for remote access. This is a brief, uncomplicated procedure documented in the *DHIAP RADIUS Supplemental Installation and Maintenance Guide (ATI Special Report IPS 00-03)*. Second, the users must be assigned to the type of remote access appropriate to their role at the facility. (From implementing the RADIUS-compliant technology, the MTF should have a documented procedure for this activity.)
- The effect on the site's IMD staff will vary with the level of responsibility carried by the site. Responsibility will be determined as part of the region/MTF planning for the installation, in concert with deciding the type of equipment to be placed there. For example, the site (e.g., region) where the central Complete (AAA-NAS) System is installed will probably be responsible for installation and ongoing maintenance of that system. For a NAS-only site, responsibility might be placed at the MTF/clinic, or it might be carried by the central site.

Table 5 provides a list of the types of activity that IMD will perform in supporting the DHIAP prototype technology, the DHIAP team's recommendation for each responsible person's level of experience and/or training, and an estimated time requirement to perform the work.

Table 5 – Task, Training, and Staffing Requirements to Support the DHIAP Technology

Support Task	Type of IMD Staff	Training/Experience Required	Estimated Effort
Prior Experience	System/Network Administrator	1. Basic router configuration 2. Windows NT Server installation and administration	N/A
Installation	System/Network Administrator ¹⁴	1. DHIAP initial training for RADIUS system administrator 2. Self-study and hands-on experience	1. 4 to 8 hours training in: <ul style="list-style-type: none">▪ Configuration of system parameters▪ General user setup▪ System maintenance 2. Eight hours (approx.)
Set up current users for RADIUS-controlled remote access	System Administrator	N/A	Varies with number of users (@2 to 5 minutes/user) to: <ul style="list-style-type: none">▪ Establish and configure AAA Access Control List▪ Enroll users into appropriate ACL groups

¹⁴ Note that a minimum of two system administrators should be trained in order to have adequate staffing backup.

DHIAP PHASE I TECHNOLOGY DEMONSTRATION

PROTOTYPE FOR REMOTE AUTHENTICATION DIAL-IN USER SERVICE (RADIUS)

Table 5 – Task, Training, and Staffing Requirements to Support the DHIAP Technology

Support Task	Type of IMD Staff	Training/Experience Required	Estimated Effort
Ongoing system and user database maintenance	System Administrator	N/A	Varies with number of users: <ul style="list-style-type: none">▪ Set up user restrictions▪ Update users' group assignments▪ Update AAA Access Control List

For all of the work outlined in **Table 5**, the *DHIAP RADIUS Supplemental Installation and Maintenance Guide (ATI Special Report IPS 00-03)* provides useful general information and instruction.

APPENDICES

APPENDIX A

Reference Materials

The following materials were used as reference materials by participants of the DHIAP Phase I effort.

- AR 380-19, Information System Security, 27 February 1998
- AR 380-53, Information Systems Security Monitoring, 29 May 1998
- MCUB-AS (25), Memorandum of Instruction: Release of Medical Information and Freedom of Information Act Processing
- MEDDAC Regulation 190-51,
- Military Health Services System (MHS) Automated Information Systems (AIS) Security Policy Manual, Version 1.0, April 1996
- Department of Defense Technical Architecture Framework Information Management, Volume 6: DoD Goal Security Architecture, Version 3.0, 30 April 1996
- Army Medical Department (AMEDD) Information Systems Security Plan (undated)
- Risk Analysis, MEDCOM Network Security Project, Prepared by Science Applications International Corporation, February 5, 1997, for Tripler Regional Medical Center
- Local policy memorandum and regulations on Personnel and Physical Security Program and Security Standards for Automation Data Processing

Note that the pending legislation and regulatory guidance of Health Insurance Portability and Accountability Act of 1996 (HIPAA), expected to be effective during 2000 and requiring compliance about two years afterwards, will also affect requirements for privacy of individually identifiable health information. It is expected that HIPAA requirements will be incorporated into requirements of the Joint Commission on Accreditation of Healthcare Organizations.

APPENDIX
B

Army Dial-in Modem Standards and Policy

Subject: [R] NETWORK SECURITY IMPROVEMENT PROGRAM (NSIP) -- ARMY

Author: Dolores Perez at MEDCOM2_FSHTX

Date: 4/27/99 9:49 AM

RTTUZYUW RUEAUSA9699 1131825-UUUU--RUERSHA.

ZNR UUUUU

R 231300Z APR 99

FM HQ WASHINGTON DC//SAIS-IAS//

***SUBJECT: NETWORK SECURITY IMPROVEMENT PROGRAM (NSIP) –
ARMY MODEM DIAL-IN STANDARDS AND POLICY.***

1. The purpose of this message is to provide standards and policy for the implementation of protected dial-in systems Army-wide. Dial-in systems can be an exploitable entry point into the information backbone. Installation DOIMs must ensure that all Army dial-in operations to include information technology functions adhere to the standards stated in this message. This message applies to the active Army, the Army National Guard, and the U.S. Army Reserve.
2. Army dial-in users will be required to migrate to an identification and authentication (I&A) system that will authenticate all dial-in operations with a unique user-id and password, that is compliant with the remote authentication dial-in user system (RADIUS) Standard, nlt one calendar year from the dtg this message. The standards for such a system are:
 - A. All dial-in operations will be authenticated with a unique user-id and password. Passwords shall be at least eight randomly generated alphanumeric characters and reflect the current Army password expiration policy of 6 months.
 - B. I&A systems supporting dial-in capabilities will migrate to the JTA compliant RADIUS standard. The RADIUS software shall be configured for accounting. Accounting logs will at a minimum show who logged in, when they logged in, and be stored for a year.

- C. All I&A servers will be protected with a host based ids. I&A server managers and DOIMs are responsible for operating and auditing the ids results.
 - D. The MACOM Information Assurance (IA) officer will be responsible for reporting the location/ip address/hardware platform and version of the os of the I&A servers to the odisc4 poc for this message.
 - E. All I&A servers will be remotely audited to ensure all Army IA standards established in this message are met. Recommend that DOIMs place I&A servers in a DMZ. The odisc4 poc this message will coordinate the remote configuration audits with the MACOM IA officer.
3. The following actions must be considered when setting up a authentication system.
- A. If necessary, users must upgrade local terminal servers to be RADIUS compliant. Cisco terminal servers running IOS 11.2 or greater are RADIUS compliant. The Army disn router program upgraded the old CISCO asm terminal servers to CISCO 5200 terminal servers. The old CISCO asm terminal servers cannot run IOS 11.2 and must be upgraded or removed from operation.
 - B. Microsoft RAS must be configured to allow tcp/ip or ipx clients access only to the local network. Care should be taken when configuring user dial-in accounts. If a dial-in system is intended to restrict access to a local network, then users will be required to log-off before attempting to access a different local network.
 - C. The Microsoft RAS must be configured to ensure that passwords are encrypted.
 - D. Microsoft remote access servers will be placed in the DMZ and must be configured for RADIUS and host-based ids.
4. DOIMS must ensure that any dial-in systems that are connected to the installation data networks, that they own or operate, adhere to these RADIUS standards. If they do not, they must be disconnected. Those systems that are not owned or operated by the post, camp or installation DOIM and are not willing or able to meet Army standards must be reported to the odisc4 poc for this msg.
5. Stand alone dial-back modems and modem systems that authenticate using RADIUS are the only allowable modems. Without aggressive action, dial-in systems and stand-alone modems will continue to be a potential backdoor for unauthorized intruders.
6. odisc4 pocs for this message are:
- A. Ltc Lundgren dsn 664-8377, email lundgl@hqda.Army.mil
 - B. Mr. Phillip Loranger dsn 327-5887, cmcl 703-607-5887, email lorangep@hqda.Army.mil
7. asc technical pocs are:
- A. Mr. Robert Manning dsn 879-8195, email manningr@hqasc.Army.mil
 - B. Mr. Peter E. Pietras, dsn 879-8195, cmcl (520) 538-8195, pietrasp@hqasc.Army.mil
 - C. Mr. Sam Dean, deans@hqasc.Army.mil, dsn 821-4987, cmcl (520) 533-4987.

APPENDIX C

Overview of IETF Internet Standard Protocol for RADIUS

RADIUS is an Internet standard protocol “for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.”¹⁵ As described in the protocol, “managing dispersed serial line and modem pools for large numbers of users can create the need for significant administrative support. Since modem pools are by definition a link to the outside world, they require careful attention to security, authorization and accounting. This can be best achieved by managing a single “database” of users, which allows for authentication (verifying user name and password) as well as configuration information detailing the type of service to deliver to the user (for example, SLIP, PPP, telnet, rlogin). Key features of RADIUS are:

- **Client/Server Model**

A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned.

RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

- **Network Security**

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an unsecure network could determine a user’s password.

¹⁵ Internet Engineering Task Force (IETF) Network Working Group document; URL for the IETF RADIUS standard (rfc 2138) is <http://www.ietf.org/rfc/rfc2138.txt>

The standard describes the protocol for “AAA,” or *Authentication, Authorization, and Accounting* of dial-in users who request access to a network and its resources.

- **Authentication** assures that a user is who he claims to be. It is accomplished by verifying the User ID and Password provided when the user initially attempts to access the network.
- **Authorization** limits the authenticated user’s access to predetermined resources. It intercepts the user’s attempt to access a network resource and verifies whether access to that resource is permitted.
- **Accounting** maintains a log of session statistics. Logging entries can include, but are not limited to, login and exit time, user IP Address, user name, Network Access Server (NAS) entry port, and denial of login privileges.

APPENDIX D

DHIAP Prototype Implementation

Equipment Configuration

Components of the prototype RADIUS-compliant system used in the DHIAP demonstration are shown in **Figure D1**. The hardware consists of an Intel-based computer, a router capable of housing 8, 16, 24, or 32 modems (as required by the site), an uninterruptible power supply (UPS), and a mobile tower rack to house them all.

The Intel-based computer is established as the RADIUS AAA Server by loading it with and configuring Windows NT Server, Internet Information Services (IIS), and CiscoSecure ACS software. The router is established as the RADIUS Network Access Server (NAS) by configuring its IOS software with commands that enable it to work with the AAA Server. The UPS is configured by installing its APC PowerChute Plus software on the NT Server (the Intel-based computer).

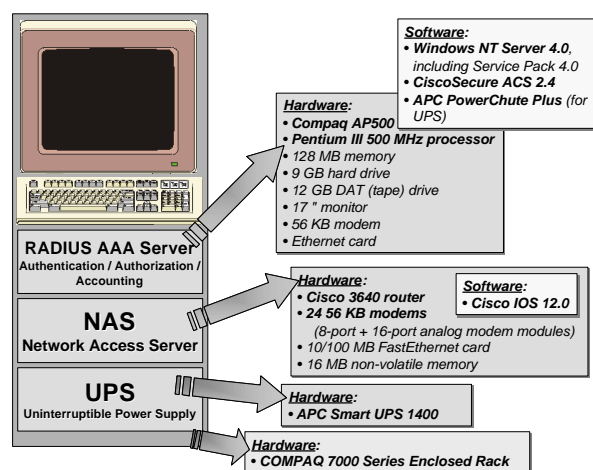


Figure D1 – Components of the DHIAP Demonstration's RADIUS-compliant System

Processing Flow

Authentication

The DHIAP demonstration's RADIUS-compliant system is designed for implementation at the point of dial-in access of each MTF's existing network infrastructure. **Figure D2** provides a diagram and brief explanation of the basic processing for authentication of a remote user. Note that, by using the region's NT Domain Controller architecture as its authority for authentication, the DHIAP approach utilizes the region's existing central resource for controlling its users' User ID/Password pairs, greatly simplifying implementation and maintenance of the RADIUS-compliant system.

Authorization

For authorization, the process that is executed each time an authenticated user requests access to a different network resource, the NAS uses the access permissions previously provided by the AAA Server during the authentication process to determine whether to permit or deny the request. Information defining the system resources that a dial-in user may access was transferred during authentication from the AAA Server's User Database to the NAS, where it is held in memory for the duration of the user's online session. The CiscoSecure software on the AAA Server permits definition of up to 99 Access Groups for the Access Control List used as the NAS authorization resource. Each Access Group is defined by the system administrator to represent a unique mix of resources offered at the site. (Note that a typical site is likely to use only 2 to 4 groups.) Besides identifying the network resources to be allowed or denied, these access permissions allow for such control features as limits on the time of day when remote login is permitted for the user and restrictions on the dial-in port from which the user may work. **Figure D3** depicts a remote dial-in session and several resources that might be available on the network, and indicates whether the user is permitted access to them. Note that all communications during the remote session pass only through the NAS after the user is authorized, no longer involving AAA Server processing.

For situations where a first-time remote user is known to the NT User Database and authorized for remote access but not yet defined in the AAA Server, the NAS is typically configured to automatically assign the user to its "default" Access Group. Resource permissions for default access are usually very limited (e.g., e-mail only). A formal procedure at the facility that involves the user, management, and system administrator would then be followed to assign the user to a different remote Access Group that offers resources more appropriate to the user's role at the facility; the user's next remote session would then be managed by the NAS in accordance with the newer entry. Note that the Access Group assignment/Access Control List entry does not necessarily grant remote users the same types of access they enjoy when working onsite. For example, a nurse who uses NT Office functions and CHCS when onsite might be denied outside access to CHCS but permitted access to NT Office functions.

Accounting

As it completes each step of the authentication process, the AAA Server records session statistics on the Accounting Log file.¹⁶ The systems administrator may customize the information that is recorded on the log, typically including for all log on attempts, both successful and failed, the user's User ID, login port, login time, and the IP address used for the session. AAA administrative software allows the system administrator to alter the log's categories of information capture as the needs of the site change. The software also allows for configuring the Accounting process to generate an automated warning when a questionable activity occurs. For instance, detection of repeated unsuccessful login attempts could generate an e-mail message or a page to a system administrator so that the suspicious activity could be investigated immediately.

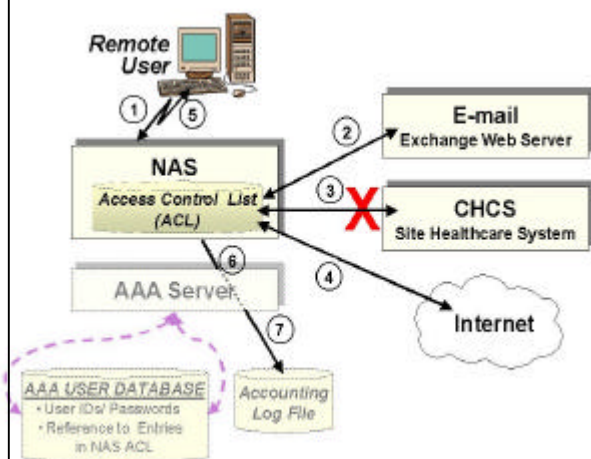
¹⁶ AAA Server logging records events related to network access. It is not related in any way to the type of logging performed in some application systems, which often records events related to user access and modification of the application's data records and data elements.

DHIAP PROTOTYPE IMPLEMENTATION

Figure D2 – AUTHENTICATION/ACCOUNTING for Remote User Access to Network Resources

The numbers used in the steps below relate to the circled numbers in the diagram to the left.

1. Remote user dials into the local site, providing User ID and Password
2. NAS accepts user input, sends User ID/Password pair to AAA Server for Authentication (password is sent in encrypted format)
3. AAA Server accesses the AAA User Database to determine whether User ID/Password pair is valid; if found and pair is valid (i.e., OK), bypass step 4 below and go to step 5
4. If User ID/Password pair is not found in the AAA User Database, AAA Server queries the NT Server for Authentication as follows:
 - 4.a. NT Server accesses NT User Database to determine whether:
 - User ID/Password pair is valid, and
 - User is authorized for remote access to network resources
 - 4.b. Based on 4a results, NT Server returns one of the following Authentication results to AAA Server:
 - OK if User ID/Password pair is valid and remote access is permitted
 - NOT OK if User ID/Password pair is valid but remote access is not permitted
 - NOT OK if User ID/Password pair is invalid
5. If result from step 3 or NT Server's result from step 4b is OK, AAA Server uses User ID to acquire the user's Access Control List reference information from AAA User Database. AAA Server sends its Authentication result to NAS as follows:
 - If OK, AAA sends an acceptance indicator and the user's Access Control List reference information to NAS
 - If NOT OK, AAA sends a rejection indicator to NAS
6. AAA Server logs the user's access request and OK/NOT OK disposition to the Accounting Log file
7. NAS concludes Authentication as follows:
 - 7.a. **USER ACCEPTED:** Based on AAA Server's Access Control List reference, NAS establishes user's Access Group for the session and proceeds to Authorization
 - 7.b. **USER REJECTED:** NAS sends rejection notification to user, terminates session

Figure D3 – AUTHORIZATION/ACCOUNTING for Remote User Access to Network Resources

The numbers used in the steps below relate to the circled numbers in the diagram to the right. In this example, authentication of the user has been completed. The user is accepted, remote access is permitted, and the Access Group permissions (known via the user's ACL entry in the NAS) allow the user to work remotely with e-mail and the Internet.

1. User requests login to the E-mail Exchange Web Server; access is permitted
2. User requests login to CHCS; request is denied
3. User requests access to the Internet; access is permitted
4. User logs off system
5. NAS sends the user's logoff statistics to AAA Server
6. AAA Server posts logoff statistics on Accounting Log file

APPENDIX
E

Acronyms

Acronym / Term	Meaning
ADL	Arthur D. Little
ATI	Advanced Technology Institute
CHCS	Composite Health Care System
CIO	Chief Information Officer
Cisco	Vendor of hardware and software used in the DHIAP demonstration
DHIAP	Defense Healthcare Information Assurance Program
DISA	Defense Information Systems Agency
DISC4	Directorate of Information Systems, Command, Control, Communications, and Computers
DOD	Department of Defense
HIPAA	Health Insurance Portability and Accountability Act of 1996
HOST	Healthcare Open Systems and Trials
IETF	Internet Engineering Task Force
IOS	Internet Operating System (Cisco's operating system)
IP	Internet Protocol
ISE	Information Security Evaluation
IT	Information Technology
LMES	Lockheed Martin Energy Systems
MEDCOM	Medical Command
MRMC	Medical Research and Material Command
MTF	Medical Treatment Facility
OSD(HA)	Office of Secretary of Defense (Health Affairs)
PC	Personal Computer
RADIUS	Remote Authentication Dial-In User Service
SEI	Software Engineering Institute
TATRC	Telemedicine and Advanced Technology Research Center
TCP	Transmission Control Protocol
TIMPO	Tri-Service Infrastructure Management Program Office
UPS	Uninterruptible Power Supply

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE April 2000		3. REPORT TYPE AND DATES COVERED Report of DHIAP Phase I Technology Demonstration, Jan 1999 - April 2000
4. TITLE AND SUBTITLE DHIAP Phase I Technology Demonstration Report: Prototype for Remote Authentication Dial-In User Service (RADIUS)			5. FUNDING NUMBERS DAMD17-99-C-9001	
6. AUTHORS L. Crane, L. Melton, J. Stinson				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) ATI 5300 International Blvd. N. Charleston, SC 29418			8. PERFORMING ORGANIZATION REPORT NUMBER ATI IPS TR 00-04	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) USAMRAA 820 Chandler St. Ft. Detrick, MD 21702-5014			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) The Defense Healthcare Information Assurance Program (DHIAP) involved demonstration of prototype information assurance technology to assess the impact on military Medical Treatment Facility (MTF) operations and ability to improve security of sensitive information. The prototype, developed and tested in a distributed laboratory and demonstrated at two MTFs within a region, is a system that meets the Remote Authentication Dial-In User Service (RADIUS) standard. This report describes the development and trials of the technology and provides an analysis of alternative approaches for implementation of RADIUS-compliant systems within the Army MTF infrastructure.				
14. SUBJECT TERMS Information Security, Information Technology, Information Assurance, Computer Security, Healthcare Information Systems, RADIUS, Network Access Security, Access Control, Dial-In			15. NUMBER OF PAGES 47	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL	